DOCKET FILE COPY ORIGINAL

# Before the Federal Communications Commission Washington, D.C. 20554

FEB 12 1998

PEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of	)	
	)	
Communications Assistance for Law	)	
Enforcement Act	)	CC Docket No. 97-213
	)	

## Ameritech Reply Comments on Notice of Proposed Rulemaking

The Ameritech Operating Companies<sup>1</sup> respectfully submit its reply comments in the Federal Communication Commission's Notice of Proposed Rulemaking issued in CC Docket No. 97-213, In the Matter of the Communications Assistance for Law Enforcement Act. In 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) which imposes certain obligations on telecommunications carriers. Specifically, CALEA requires telecommunications carriers subject to the Act to expeditiously isolate, intercept and deliver wire and electronic communications to law enforcement, and to expeditiously isolate and enable law enforcement access to call identifying information that is reasonably available.

On October 10, 1997 the Federal Communications Commission issued a Notice of Proposed Rulemaking regarding the implementation of the Communications Assistance for Law Enforcement Act (CALEA). The FCC's NPRM focused primarily on the following issues: 1) which telecommunications carriers are covered under CALEA; 2) establishment of the proper internal procedures under which carriers initiate

<sup>&</sup>lt;sup>1</sup> The Ameritech Operating Companies are Ameritech Illinois, Ameritech Indiana, Ameritech Michigan, Ameritech Ohio, and Wisconsin Bell, Inc. d/b/a Ameritech Wisconsin.

surveillance's for law enforcement; and 3) what factors should be considered under the 'reasonably achievable' standard.<sup>2</sup>

Many parties provided extensive comments on the FCC's' proposed rules. For the most part, parties were in agreement that the telecommunications carriers subject to CALEA should be broadly defined. In addition, parties agreed that the FCC did not have jurisdiction to require that information services be subject to CALEA compliance requirements, regardless of the type of carrier providing them. Similarly, a majority of the parties agreed that the FCC should establish simple and straightforward rules relating to the internal procedures for carriers to initiate surveillance's for law enforcement. In fact, some parties argued that the FCC's proposed rules were unnecessary since carriers have been effectively initiating surveillance's for law enforcement for years, without the need for government oversight. These parties suggest that, at the most, the FCC should only require carriers to certify that their internal procedures meet the requirements of the law, similar to the FCC's proposal for small carriers.<sup>3</sup> Finally, there was considerable discussion regarding the criteria for requesting an extension of time under Section 107 of CALEA as well as the criteria for evaluating whether compliance with the capability requirements under Section 109 was 'reasonably achievable.' In this regard, a distinction was made between the criteria necessary to grant an extension of time under Section 107,

<sup>&</sup>lt;sup>2</sup> In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, Notice of Proposed Rulemaking, released October 10, 1997, at Paragraph 9.

<sup>&</sup>lt;sup>3</sup> See for example Comments filed by GTE Service Corporation, SBC Communications, Inc.

and the criteria to establish that compliance for certain equipment is not 'reasonably achievable.'

Ameritech would like to focus its reply comments on three areas: 1) information services and CALEA; 2) internal carrier procedures for initiating surveillance activities for law enforcement; and 3) relief from CALEA compliance under Section 107 or Section 109.

#### A. <u>Information Services</u>

Several parties, like Ameritech, point out that the CALEA legislation specifically excludes "information services" from the requirement to comply with CALEA.<sup>5</sup>

Congress made no distinction between information services provided by common carriers and information services provided exclusively by information service providers.

Consequently, the FCC's proposal to require CALEA compliance for those information services provided by common carriers is clearly beyond the authority granted by the law. Thus, the FCC cannot adopt this proposed rule.

#### B. <u>Internal Procedures</u>

Many parties questioned the FCC's proposed rules for internal procedures for carriers initiating surveillance activities for law enforcement. Most carriers stated that the FCC's proposed rules were unduly burdensome. Specifically, carriers questioned the need for extensive record keeping at all levels of surveillance activities, by all parties

<sup>&</sup>lt;sup>4</sup> See for example Comments filed by Ameritech Corporation.

<sup>&</sup>lt;sup>5</sup> See for example Comments filed by USTA, US West, Inc., and American Civil Liberties Union, Electronic Privacy Information Center and Electronic Frontier Foundation.

regardless of whether the person has any knowledge that a surveillance activity is being initiated.<sup>6</sup> The FBI, on the other hand, not only substantially supports the FCC's proposed rules but also provided further comment on the procedures carriers should be required to adopt.<sup>7</sup>

While Ameritech generally supports the FCC's proposed rules for internal procedures for initiating surveillance activities, the FCC should not adopt several of the additional requirements proposed by the FBI. At the outset, Ameritech disagrees with the FBI's statement that centralized implementation of surveillance activity causes any hardship on law enforcement. Ameritech has found that in its region, security centralization has provided more efficient and uniform response to law enforcement's requests. As for the FBI's specific suggestions, the FBI argues first that carriers should not look beyond a facially valid order prior to initiating an intercept. In this regard, the FBI disagrees with the FCC's proposal that "appropriate authorization" under Section 229(b)(1) of CALEA refers to the necessary authorization the carrier provides to the employees prior to implementing a surveillance. The FBI interprets this requirement to require carriers to review de novo any court order, warrant or subpoena prior to initiating a surveillance.

<sup>&</sup>lt;sup>6</sup> See for example Comments filed by GTE Corporation, US West, Inc., Teleport Communications Group, Inc., and Airtouch Communications, Inc.

<sup>&</sup>lt;sup>7</sup> See Comments filed by the Federal Bureau of Investigation (FBI), at pages 15-35.

<sup>&</sup>lt;sup>8</sup> FBI Comments at paragraph 32.

While Ameritech agrees with the FBI's interpretation that "appropriate authorization" refers to the legal document supporting the surveillance, Ameritech disagrees with the FBI's proposal that a carrier's review is limited to determining whether the court order, warrant or subpoena is valid on its face. Specifically, carriers are only protected from liability for initiating and assisting law enforcement in surveillance activities if the carrier has a "good faith reliance" on the court order, warrant or subpoena.

18 U.S.C. section 2520(d). Even the FBI mentions this standard in its comments. Thus, in order for a carrier to meet this standard of care, the carrier must have a reasonable basis on which to believe that the court order, warrant, subpoena, or law enforcement request is valid. A facial or cursory review of the order, as suggested by the FBI, is not sufficient to meet this standard. Thus while the FCC should establish that "appropriate authorization" under Section 229(b)(1) means the court order, warrant or subpoena, the FCC should also clarify that carriers must have a reasonable basis on which to rely on that authorization.

Second, the FBI proposes that carriers should be required to perform background checks for those employees that are involved in implementing electronic surveillance. In addition, the FBI proposes that these background checks be placed in employees' personnel files in case of compromises of security. This proposal is overburdensome and unnecessary, as well as intrusive upon the carrier's internal personnel policies. Carriers are responsible for hiring employees that are capable and trustworthy to perform the functions involved in electronic surveillance. In a substantial majority of cases, a

<sup>9</sup> <u>Id</u>. at paragraph 35, note 23.

<sup>&</sup>lt;sup>10</sup> <u>Id</u>. at paragraphs 37-41.

carrier's employees are former law enforcement officers themselves. A carrier should not be required to perform a background check on all of its employees designated to be involved in electronic surveillance. The FBI provides no justification for this intrusive policy. Should the FBI feel the need to perform such checks on carriers' designated employees then the FBI should perform the background checks at its <u>own</u> expense.

Third, the FBI supports the FCC's proposal to have carriers report compromises of surveillance activities to the FCC in addition to the FBI. A number of parties, including Ameritech, believe that not only is this an unnecessary burden, but there is an issue regarding whether carriers even have the authority to provide such information to the FCC under the current law. Carriers have been successfully assisting law enforcement in their electronic surveillance activities for years. There is no information in the record that establishes that carriers have not been performing these functions or that they have not sufficiently informed law enforcement when any surveillance activities have been compromised. Moreover, there is no demonstration that providing such information to the FCC, in addition to the affected law enforcement agency, will serve to more effectively protect surveillance activities. Thus, the FCC should not adopt this proposal.

<sup>11</sup> Id. at paragraph 45.

<sup>&</sup>lt;sup>12</sup> See for example Comments filed by Ameritech Corporation, Airtouch Communications, Inc., and US West, Inc.

<sup>&</sup>lt;sup>13</sup> See Ameritech Comments at note 4.

Fourth, the FBI proposes that surveillance activities be implemented within two (2) hours of receipt of the court order, warrant or subpoena. The FBI also proposes that a similar two (2) hour timeframe be established for reporting to law enforcement any compromises or malfunctions of surveillance activities. <sup>14</sup> In addition, the FBI proposes that carriers have personnel available seven days a week, twenty-four hours a day to respond to surveillance requests.

While Ameritech generally has personnel available seven days a week, twentyfour hours a day, the FCC should not adopt the FBI's suggestion that surveillance
activities be implemented within two hours, and that compromises of such activities be
reported to law enforcement in two hours. These timeframes are neither necessary nor
workable. In this regard, there are a substantial number of administrative and network
issues that need to be performed when implementing interceptions. Carriers, for
example, need to identify: 1) the target number; 2) the proper switch and its location; and
3) the appropriate type of intercept that needs to be performed. These functions do not
even include the additional recordkeeping and administrative requirements proposed by
the FCC and the FBI. While Ameritech fully acknowledges the importance of
electronic surveillance, in almost all circumstances for surveillance activities, life and

-

<sup>&</sup>lt;sup>14</sup> See FBI Comments at paragraphs 70-71.

<sup>&</sup>lt;sup>15</sup> In fact, in direct contrast to its earlier suggestions for substantial recordkeeping and administrative policies and in support of its two hour timeframe the FBI states '[t]he more cumbersome a carrier's implementation procedure, the greater the likelihood that investigations will be hampered by unnecessary delays." FBI Comments at paragraph 69.

death is not held in the balance.<sup>16</sup> Rather, court orders, warrants, and subpoenas can be implemented within the normal course of business.

Consequently, absent exigent circumstances, the FCC should require the implementation of court orders, warrants and subpoenas within twenty-four (24) hours of receipt. The FBI argues that delays in the implementation of surveillance activities result in the possibility of loss of evidence because the target has moved on or the order has expired. The proposed 24-hour timeframe will more than suffice to meet these concerns. Also, it is a reasonably efficient timeframe necessary in which to initiate timely and effective surveillance activities.

Finally, in its comments on internal procedures, the FBI states that carriers that allow third parties access to switches should be required to maintain records that include the date, time, purpose and identity of the third party personnel involved for each access. This comment overlooks a significant issue that has yet to be addressed -- the issue of the impact of the requirement that carriers provide unbundled local switching to other telecommunications carriers under the new interconnection provisions, Sections 251 and 252 of the Telecommunications Act of 1996. Implementation of unbundled local switching is based on the interconnection negotiations and/or arbitrations between local exchange carriers and telecommunications providers, which is a dynamic process. As a

<sup>&</sup>lt;sup>16</sup> In those instances in which life and death are at stake, Ameritech has and will continue to respond accordingly.

<sup>&</sup>lt;sup>17</sup> See FBI Comments at paragraph 8.

<sup>&</sup>lt;sup>18</sup> See FBI Comments at paragraph 68.

result, there is no concrete information within the industry from which to determine whether this proposal by the FBI is workable.

C. Extensions of Compliance Requirements under Sections 107 and 109 of CALEA

The FBI states that there is no need for the FCC to consider specific rules regarding requests for extension of time to comply with CALEA under Section 107 of the Act. The FBI accurately points out that the criteria to establish whether technical capability is available in order for carriers to meet the compliance dates under Section 107 is substantially different than the criteria necessary to determine whether it is reasonably achievable for a carrier to implement the CALEA compliance solution on "equipment, facility, or service installed or deployed after January 1, 1995" under Section 109. The FBI argues further that there may be a network-based, non-switched based solution that would enable carriers to meet the technical capability requirements of CALEA that would preclude an extension of time.

The FCC will need to deal with the issue of extensions of time under Section 107 within a short period of time. In a CALEA Implementation Report (Report) provided to Chairman, Harold Rogers, House Appropriations Subcommittee for the Departments of Commerce, Justice, and State, on January 26, 1998, the FBI has provided all the necessary information to support a blanket extension of time to all carriers under Section 107 of the Act. In the Report, the FBI details the information manufacturers have provided about the availability of the CALEA solution. This Report demonstrates that

<sup>&</sup>lt;sup>19</sup> <u>Id</u>. at paragraph 97.

not one switch manufacturer can provide a capability solution by October 25, 1998. Moreover, it shows that only a few of the switch manufacturers can provide a 'partial solution' by late 1998 and early 1999, while one switch manufacturer will provide a complete solution in late 1999.<sup>20</sup>

The availability of these switched-based solutions within the designated timeframe, of course, presupposes that there are no technical issues that need to be resolved, and that the switch manufacturers can immediately begin to build the solution based on the interim standard. But, in fact, there are technical issues which the FCC is going to have to resolve. Currently, the industry and the FBI are at an impasse regarding approximately eleven capabilities; the industry argues that these capabilities are not required by CALEA, while the FBI argues that these capabilities are required by CALEA. The Cellular Telecommunications Industry Association has already requested that the FCC resolve this deadlock in an October, 1997 filing. Surely, carriers cannot be found to be in violation of CALEA for not meeting the FBI requirements, when CALEA does not grant the FBI the authority to establish a technical standard, and there remains a substantial disagreement as to what is required under the law.

Furthermore, the FBI's argument that no extension of time is needed for CALEA compliance because a network-based, non-switched based solution might be available by October, 1998, is optimistic at best. In its January 26, 1998 Report to Congress, the FBI

<sup>&</sup>lt;sup>20</sup> See CALEA Implementation Report, January 26, 1998 at page 18.

In this regard, there is significant disagreement between the parties as to the actual requirements of CALEA capability. The result of this disagreement was the adoption of an "interim" standard, which does not resolve the issue of what CALEA capability actually requires.

states that Bell eMergis claims that it can provide a CALEA solution by October, 1998.<sup>22</sup> However, as yet no U.S. carrier has deployed this non-switched-based solution in its network to determine whether this solution provides all the necessary CALEA capabilities in an efficient and effective manner. In this regard, while the switch manufacturers are building the capability that will function within the manufacturer's own switch, Bell eMergis' solution must be built into carriers' networks in order to interact with the switches of all manufacturers. In fact, Ameritech worked with Bell eMergis to determine whether Bell eMergis' solution was viable within the Ameritech network. Ameritech concluded that it would take substantial work to have Bell eMergis' solution incorporated into its network, and that some of that work would have to be done directly with the switch manufacturers.<sup>23</sup> Ameritech provided to Bell eMergis a written summary of its conclusions, and informed the FBI of its conclusion not to move forward with the Bell eMergis solution in December, 1997.<sup>24</sup> While Ameritech does not speak for the entire telephone industry, since no other U.S. carrier has yet to evaluate this solution, it seems premature for the FBI to indicate that this network-based solution might be available in time for carriers to deploy it by October, 1998.

\_

<sup>&</sup>lt;sup>22</sup> CALEA Implementation Report at 3.

This fact contradicts the FBI's statement that a network-based solution does not require a switch manufacturer to make internal switch software or hardware modifications, and carriers need to only make minor modifications to their end office switches. See CALEA Implementation Report at 7.

<sup>&</sup>lt;sup>24</sup> Letter to Mr. Michael Warren, Section Chief, CALEA Implementation Section, Federal Bureau of Investigations, from Mr. Don Auble, Director - CALEA Project Manager, Ameritech Corporation, dated December 16, 1997.

Thus, until there is a proven technical solution -- either a switch-based or non-switched based solution -- available to all carriers, the compliance date of October, 1998 cannot be achieved. And, since the FBI's report to Congress makes clear that no such solution will be available by October, 1998, the FCC must grant an extension of time under Section 107 of the Act.<sup>25</sup>

With regard to the criteria for determining whether compliance is 'reasonably achievable' under Section 109 of the Act, the Act requires that the FCC weigh a number of different factors. The FBI argues, however, that the "effect on public safety and national security" factor should be given paramount weight in the FCC's determination of whether compliance is 'reasonably achievable.' Nevertheless, as noted by both the FCC and the FBI, Congress *carefully balanced* CALEA's requirements among three important policies: 1) to preserve a "narrowly focused" capability of law enforcement to carry out authorized intercepts; 2) to protect the privacy rights and needs of the American public in the face of increasingly revealing technologies; and 3) to avoid restricting the development of communications services and technologies which benefit the public. In seeking to balance those policies, Congress established a range of criteria for the FCC to consider when determining whether a carrier should be relieved of upgrading its equipment because the upgrade is not 'reasonably achievable.' Consequently, the FCC

<sup>&</sup>lt;sup>25</sup> Another issue which is critical for effective CALEA compliance is the actual capacity of simultaneous surveillances carriers will have to provide to law enforcement. At this time, the FBI has not released its final notice of the capacity requirement, with which carriers must comply with three (3) years of the release of the final rule.

<sup>&</sup>lt;sup>26</sup> See FBI Comments at paragraph 96.

<sup>&</sup>lt;sup>27</sup> NPRM at paragraph 5, and FBI Comments at paragraph 10.

needs to consider all these factors when making its determination under Section 109 and should not deem one factor in particular to be paramount.

#### D. Conclusion

Ameritech respectfully submits these Reply Comments, and requests the FCC to modify its proposed rules and regulations as requested above and in Ameritech's Comments.

Respectfully submitted,

Barbara J. Kern

Counsel

**Ameritech Corporation** 

2000 West Ameritech Center Drive

Room 4H74

Hoffman Estates, IL 60196

(847) 248-6077

February 12, 1998

### **CERTIFICATE OF SERVICE**

I, Audrey L. Hankel, do hereby certify that a copy of the Ameritech Reply Comments on Notice of Proposed Rulemaking has been mailed this 12th day of February, 1998, by first-class mail, postage prepaid, to parties on the attached service list.

By: Audrey L. Hankel

#### SERVICE LIST

ROBERT S. FOOSANER
LAWRENCE R. KREVOR
LAURA L. HOLLOWAY
NEXTEL COMMUNICATIONS, INC.
SUITE 425
1450 G. STREET, NW
WASHINGTON, D.C. 20005

BARRY STEINHARDT
A. CASSIDY SEHGAL
WILLIAM J. BRENNAN FELLOW
AMERICAN CIVIL LIBERTIES UNION
18TH FLOOR
125 BROAD STREET
NEW YORK, NY 10004

MARK C. ROSENBLUM
AVA B. KLEINMAN
SETH S. GROSS
ROOM 3252J1
295 NORTH MAPLE AVENUE
BASKING RIDGE, NJ 07920

ELECTRONIC PRIVACY INFORMATION CENTER SUITE 301
666 PENNSYLVANIA AVENUE, SE
WASHINGTON, DC 20003

ROSEANNA DE MARIA
AT&T WIRELSS SERVICES
ROOM 1731
32 AVENUE OF THE AMERICAS
NEW YORK, NY 10013

ELECTRONIC FRONTIER FOUNDATION SUITE 725 1550 BRYANT STREET SAN FRANCISCO, CA 94103-4832

KEVIN C. GALLAGHER 306° COMMUNICATIONS COMPANY 8725 WEST HIGGINS ROAD CHICAGO, IL 60631 PETER M. CONNOLLY
UNITED STATES CELLULAR CORPORATION
KOTEEN & NAFTALIN
1150 CONNECTICUT AVENUE, N.W.
WASHINGTON, DC 20036

ELIZABETH R. SACHS, ESQ.
LUKAS, MC GOWAN, NACE & GUTIERREZ
SUITE 1200
1111 19TH STREET, N.W.
WASHINGTON, DC 20036

JAMES T. ROCHE
GLOBECAST NORTH AMERICA, INC.
SUITE 880
400 NORTH CAPITOL STREET, N.W.
WASHINGTON, DC 20001

HENRY M. RIVERA, LARRY S. SOLOMON,
J. THOMAS NOLAN
M. TAMBER CHRISTIAN
METRICOM, INC.
GINSBURG, FELDMAN & BRESS, CHTD.
1250 CONNECTICUT AVENUE, N.W.
WASHINGTON, DC 20036

MARY MC DERMOTT, LINDA KENT, KEITH TOWNSEND, HANCE HANEY USTA SUITE 600 1401 H STREET, N.W. WASHINGTON, DC 20005

ERIC W. DE SILVA STEPHEN J. ROSEN WILEY, REIN & FIELDING 1776 K STREET, NW WASHINGTON, DC 20006 MARK J. GOLDEN
MARY E. MADIGAN
PERSONAL COMMUNICATIONS INDUSTRY
ASSOCIATION
SUITE 700
500 MONTGOMERY STREET
ALEXANDRIA, VA 22314-1561

MICHAEL K. KURTIS
JEANNE W. STOCKMAN
KURTIS & ASSOCIATES, PC
SUITE 600
2000 M STREET, NW
WASHINGTON, DC 20036

WILLIAM L. ROUGHTON, JR.

PRIMECO PERSONAL COMMUNICATIONS, L.P.

SUITE 320 SOUTH

601 13TH STREET

WASHINGTON, DC 20005

CARESSA D. BENNET
DOROTHY E. CUKIER
RURAL TELECOMMUNICATIONS GROUP
BENNET & BENNET, PLLC
SUITE 500
1019 19TH STREET, NW
WASHINGTON, DC 20036

CAROLE C. HARRIS
CHRISTINE M. GILL
ANNE L. FRUEHAUF
SOUTHERN COMMUNICATIONS SERVICES
MC DERMOTT, WILL & EMERY
600 THIRTEENTH ST, N.W.
WASHINGTON, DC 20005

STUART POLIKOFF
LISA M. ZAINA
OPASTCO
SUITE 700
21 DUPONT CIRCLE NW
WASHINGTON, DC 20036

JUDITH ST. LEDGER-ROTY
PAUL G. MADISON
PAGING NETWORK, INC.
KELLEY DRYE & WARREN, LLP
5TH FLOOR
1200 19TH STREET, NW
WASHINGTON, DC 20036

M. ROBERT SUTHERLAND THEORDORE R. KINGSLEY BELLSOUTH CORPORATION SUITE 1700 1155 PEACHTREE STREET, NE ATALNTA, GA 30309-3610

J. LLOYD NAULT, II BELLSOUTH TELECOMMUNICATIONS, INC. 4300 BELLSOUTH CENTER 675 WEST PEACHTREE STREE, NE ATANTA, GA 30375

MICHAEL P. GOGGIN BELLSOUTH CELLULAR CORP. SUITE 910 1100 PEACHTREE STREET, NE ATLANTA, GA 30309-4599

JAMES D. ELLIS, ROBERT M. LYNCH DURWARD D. DUPRE, LUCILLE M. MATES FRANK C. MAGILL SBS COMMUNICATIONS INC. . ROOM 1258 175 EAST HOUSTON SAN ANTONIO, TX 78205

JOHN T. SCOTT, III BELL ATLANTIC MOBILE, INC. CROWELL & MORING LLP 1001 PENNSYLVANIA AVENUE, NW WASHINGTON, DC 20004

RICHARD C. BARTH MARY E. BROONER MOTOROLA, INC. SUITE 400 1350 I STREET, NW WASHINGTON, DC 20005

STEWART A. BAKER, THOMAS M. BARBA KATHLEEN Q. ABERNATHY MAURY D. SHENK, L. BENJAMIN EDERINGTON MOTOROLA, INC. STEPTOE & JOHNSON LLP 1330 CONNECTICUT AVENUE, NW WASHINGTON, DC 20036

DAVID A. GROOS, DONNA L. BETHEA AIR TOUCH COMMUNICATIONS, INC. 1818 N STREET, NW WASHINGTON, DC 20036

RICHARD MC KENNA, HOE03J36 GTE SERVICE CORPORATION P. O. BOX 152092 IRVING, TX 75015-2092

GAIL L. POLIVY GTE SERVICE CORPORATION SUITE 1200 1850 M STREET, NW WASHINGTON, DC 20036

STEWART A. BAKER, THOMAS M. BARBA GRANT SEIFFERT
BRENT H. WEINGARDT MATTHEW J. FLAN
L. BENJAMIN EDERINGTON TELECOMMUNICTION
TELECOMMUNICTIONS INDUSTRY ASSOC. SUITE 315
STEPTOE & JOHNSON LLP 1201 PENNSYLVAN
1330 CONNECTICUT AVENUE, NW WASHINGTON, DC
WASHINGTON, DC 20036

GRANT SEIFFERT

MATTHEW J. FLANIGAN

TELECOMMUNICTIONS INDUSTRY ASSOC.

SUITE 315

1201 PENNSYLVANIA AVENUE, NW

WASHINGTON, DC 20004

KATHRYN M. KRAUSE
EDWARD M. CHAVEZ
US WEST, INC.
SUITE 700
1020 19TH STREET, NW
WASHINGTON, DC 20036

DAN L. POOLE
JOHN H. HARWOOD II, SAMIR JAIN
US WEST, INC.
WILMER, CUTLER & PICKERING
2445 M STREET, NW
WASHINGTON, DC 20037

TERESA MARRERO
TELEPORT COMMUNICATIONS GROUP INC.
TWO TELEPORT DRIVE
STATEN ISLAND, NY 10311

EMILIO W. CIVIDANES
OMNIPOINT COMMUNICATIONS, INC.
PIPER & MARBURY, LLP
1200 19TH STREET, NW
WASHINGTON, DC 20036

CAROLYN G. MORRIS
US DEPT. OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
J. EDGAR HOOVER BUILDING
935 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20535

JERRY BERMAN, DANIEL J. WEITZMER
JAMES X. DEMPSY
CENTER FOR DEMOCRACY AND TECHNOLOGY
1634 I STREET, NW
WASHINGTON, DC 20006

STANTON MC CANDLIS
ELECTRONIC FRONTIER FOUNDATION
SUITE 725
1550 BRYANT STREET
SAN FRANCISCO, CA 94103-4832

ANDY ORAM

COMPUTER PROFESSIONALS FOR SOCIAL

RESPONSIBILITY
P.O. BOX 717

PALO ALTO, CA 94302

MICHAEL ALTSCHUL
RANDALL S. COLEMAN
CELLULAR TELECOMMUNICATIONS
INDUSTRY ASSOCIATION
SUITE 200
1250 CONNECTICUT AVE., NW
WASHINGTON, DC 20036